# WatchGuard QMSv

# Setup Guide

WatchGuard Quarantine Management Server

# Copyright and Patent Information

Copyright© 2010–2013 WatchGuard Technologies, Inc. All rights reserved.

WatchGuard, the WatchGuard logo, LiveSecurity, and any other mark listed as a trademark in the "Terms of Use" portion of the WatchGuard Web site that is used herein are either registered trademarks or trademarks of WatchGuard Technologies, Inc. and/or its subsidiaries in the United States and/or other countries. All other trademarks are the property of their respective owners.

Printed in the United States of America.

Revised: November 13, 2013

Complete copyright, trademark, patent, and licensing information can be found in the WatchGuard product documentation. You can find this document online at:
http://www.watchguard.com/help/documentation/

# Notice to Users

Information in this guide is subject to change without notice. Updates to this guide are posted at:

http://www.watchguard.com/help/documentation/

Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of WatchGuard Technologies, Inc.

## ABOUT WATCHGUARD

WatchGuard offers affordable, all-in-one network and content security solutions that provide defense-in-depth and help meet regulatory compliance requirements. The WatchGuard XTM line combines firewall, VPN, GAV, IPS, spam blocking and URL filtering to protect your network from spam, viruses, malware, and intrusions. The new XCS line offers email and web content security combined with data loss prevention. WatchGuard extensible solutions scale to offer right-sized security ranging from small businesses to enterprises with 10,000+ employees. WatchGuard builds simple, reliable, and robust security appliances featuring fast implementation and comprehensive management and reporting tools. Enterprises throughout the world rely on our signature red boxes to maximize security without sacrificing efficiency and productivity.

For more information, please call 206.613.6600 or visit www.watchguard.com.

## ADDRESS

505 Fifth Avenue South
Suite 500
Seattle, WA 98104

## SUPPORT

www.watchguard.com/support
U.S. and Canada +877.232.3531
All Other Countries +1.206.521.3575

## SALES

U.S. and Canada +1.800.734.9905
All Other Countries +1.206.613.0895

# WatchGuard QMSv Setup

The WatchGuard® Quarantine Management Server (QMS) directs spam messages from a WatchGuard® XCS device to a local quarantine area on the QMS that provides spam storage for each individual user in your organization. When spam is filtered and processed, occasionally, a false positive (a legitimate email classified as spam) result can occur. The QMS allows end users to manage their own quarantined messages to identify and release any false positives from the quarantine, and to delete messages that are actually spam.

The QMS provides performance improvements to the integrated quarantine services on the WatchGuard XCS device. Quarantined spam is stored on a separate system, which decreases the processing load and amount of disk space used on the XCS device.

WatchGuard QMSv provides all the features of our WatchGuard QMS technology optimized for a VMware virtual machine environment. This guide introduces the WatchGuard QMSv and provides detailed information on how to configure your virtual environment and install the QMSv software.

## WatchGuard QMSv Documentation

You can use the online help manual for the majority of your documentation needs. To access the online help, from the Web UI, select **Support > Online Manual**.

You can view and download the most current documentation for the WatchGuard QMS on the WatchGuard Product Documentation page:

http://www.watchguard.com/help/documentation

# Installation Prerequisites

These sections describe the installation prerequisites for QMSv on VMware and Microsoft Hyper-V.

## VMware

You must install the QMSv virtual device in a VMware environment that meets these requirements.

### VMware

- To install an QMSv virtual device, you must have a VMware vSphere Hypervisor/ESXi v4.1 Update 2 (or later version) host installed on any supported server hardware.

**Note**

Make sure your VMware vSphere/ESXi software is updated to the latest patch level.

- You must also install the VMware vSphere Client on a supported Windows computer to manage the virtual machines on your VMware host.
- VMware Tools is installed by default with the QMSv virtual device. VMware Tools is a suite of utilities that enhances and improves the performance and management of the virtual machine, and includes the ability to cleanly power off or reset the guest operating system software from the host system.

### Hardware

- The hardware requirements for QMSv are the same as the hardware requirements for VMware vSphere Hypervisor/ESXi. For information about VMware hardware compatibility, see the VMware Compatibility Guide at: http://www.vmware.com/resources/compatibility/search.php
- WatchGuard QMSv requires that your host hardware supports Intel Virtualization Technology (Intel VT) or AMD Virtualization (AMD-V) and has these options enabled in the host system BIOS.
  - For more information about Intel VT compatibility, see the Intel Virtualization Technology List at: http://ark.intel.com/VTList.aspx
  - AMD-V is supported in all K8 AMD (Athlon 64) processors from revision F, and all newer processors support AMD-V technology.

### Features Not Supported

These features are not supported for use with WatchGuard QMSv on VMware:

- Network storage disks for the virtual host are not supported.
- QMSv does not support vMotion for virtual device migration between VMware hosts.
- QMSv console options:
  - **Serial console** — This feature is redundant with the physical host system serial console.
  - **UPS configuration** — UPS communications must be configured on the physical host system.

# Recommended Resource Allocation

WatchGuard QMSv performance is heavily dependent on CPU, memory, and disk resources. Resources are shared between all virtual machines on a virtual host, and you must make sure that enough resources are available to the QMSv virtual machine. To enable all functionality and provide optimal performance for your QMSv virtual mchine, you must allocate these resources:

| | Minumum | Maximum |
|---|---|---|
| **Virtual CPUs** | 1 | 16 |
| **Memory** | 2 GB | 4 GB |
| **Network Adapters** | 1 | 4 |
| **OS Disk space (Fixed)** | 24 GB | 24 GB |
| **Data Disk Space** | 80 GB | 256 GB |

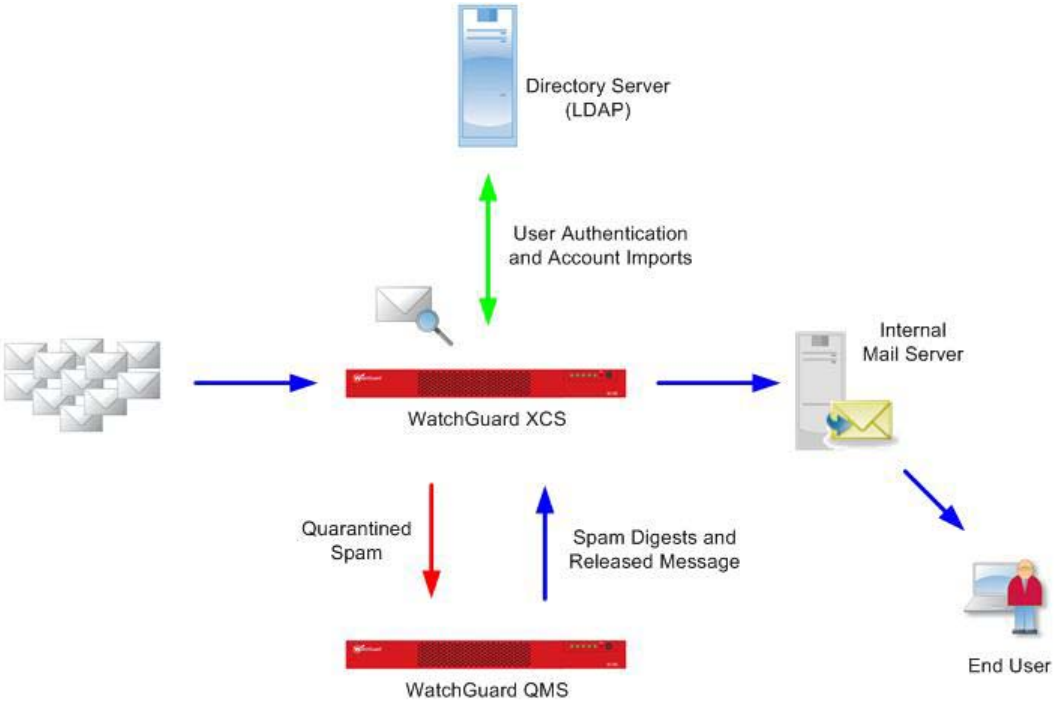
For information about how to add resources for a VMware virtual machine, see "VMware Virtual Machine Resource Allocation" on page 10.

For information on monitoring VMware resource usage, see "Resource Monitoring on VMware" on page 18.

# Deployment

With a basic internal deployment, the WatchGuard QMS is installed on the same network as the WatchGuard XCS. Incoming mail is processed by the WatchGuard XCS and any spam to be quarantined is redirected from the WatchGuard XCS to the WatchGuard QMS.

Spam digest notifications and released messages from the quarantine are delivered through the WatchGuard XCS to the internal mail servers, where they are received by the end user. End users can log in to the WatchGuard QMS to manage their specific quarantine settings, select the language template for their spam digest message, and manage their trusted and blocked senders lists.



# VMware Installation

## Before You Begin

To prepare for your installation, make sure you have these items:

- VMware vSphere Hypervisor/ESXi 4.1 Update 2 (or later version) host installed on a supported server platform.
- VMware vSphere 4.1 (or later version) client installed on a Windows computer
- WatchGuard QMSv OVF template
  *The file name is qmsv-<version>.ova, where <version> is the QMS version.*

Download the QMSv OVF template file from the **Articles and Software** section of the WatchGuard Portal at www.watchguard.com.

## Installation Overview

To complete initial installation you must perform these procedures described in the subsequent sections:

1. In the VMware vSphere client, deploy the QMSv OVF template file to the VMware host.
2. Perform any resource allocation (CPU, memory, disk, network) modifications on the VMware host.
3. Power on the QMSv virtual device.
4. Connect to the QMSv device to run the Setup Wizard.

## Time Synchronization Considerations

The WatchGuard QMSv OVF template automatically installs the VMware Tools utility software. VMware Tools is a suite of utilities for managing your virtual device, and includes a time synchronization service that synchronizes with the host system time. This service is disabled by default.

We recommend that you use the WatchGuard QMSv NTP settings to configure an NTP server, and keep the VMware Tools time synchronization service disabled. These services must not be enabled and running at the same time.

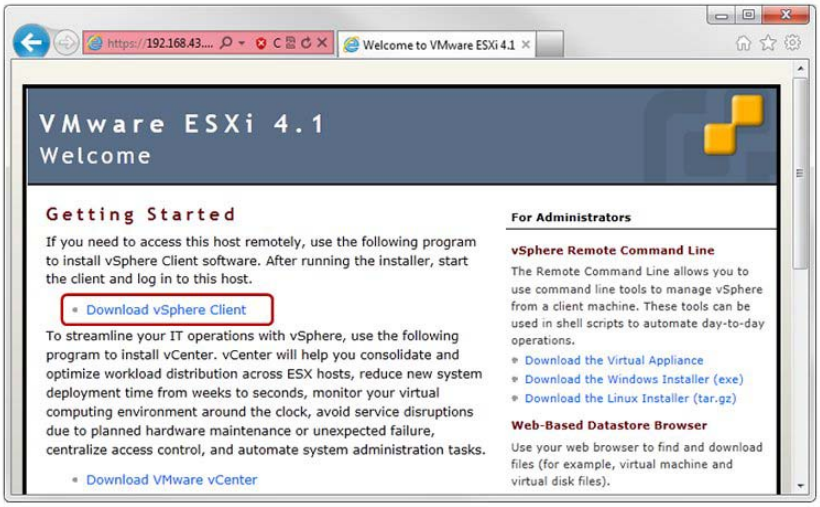
# Installation

Perform the following steps to install WatchGuard QMSv on a VMware host

## Install the VMware vSphere Client

To install the vSphere client:

1. Launch a web browser on your computer and type the IP address or host name of the VMware host server as the URL in the location bar.


https://192.168.43....
Welcome to VMware ESXi 4.1
VMware ESXi 4.1
Welcome
Getting Started
If you need to access this host remotely, use the following program to install vSphere Client software. After running the installer, start the client and log in to this host.
Download vSphere Client
To streamline your IT operations with vSphere, use the following program to install vCenter. vCenter will help you consolidate and optimize workload distribution across ESX hosts, reduce new system deployment time from weeks to seconds, monitor your virtual computing environment around the clock, avoid service disruptions due to planned hardware maintenance or unexpected failure, centralize access control, and automate system administration tasks.
Download VMware vCenter
For Administrators
vSphere Remote Command Line
The Remote Command Line allows you to use command line tools to manage vSphere from a client machine. These tools can be used in shell scripts to automate day-to-day operations.
Download the Virtual Appliance
Download the Windows Installer (exe)
Download the Linux Installer (tar.gz)
Web-Based Datastore Browser
Use your web browser to find and download files (for example, virtual machine and virtual disk files).

2. To download and install the vSphere Client, click **Download vSphere Client**.

## Connect to the VMware Host

To connect to the VMware host:

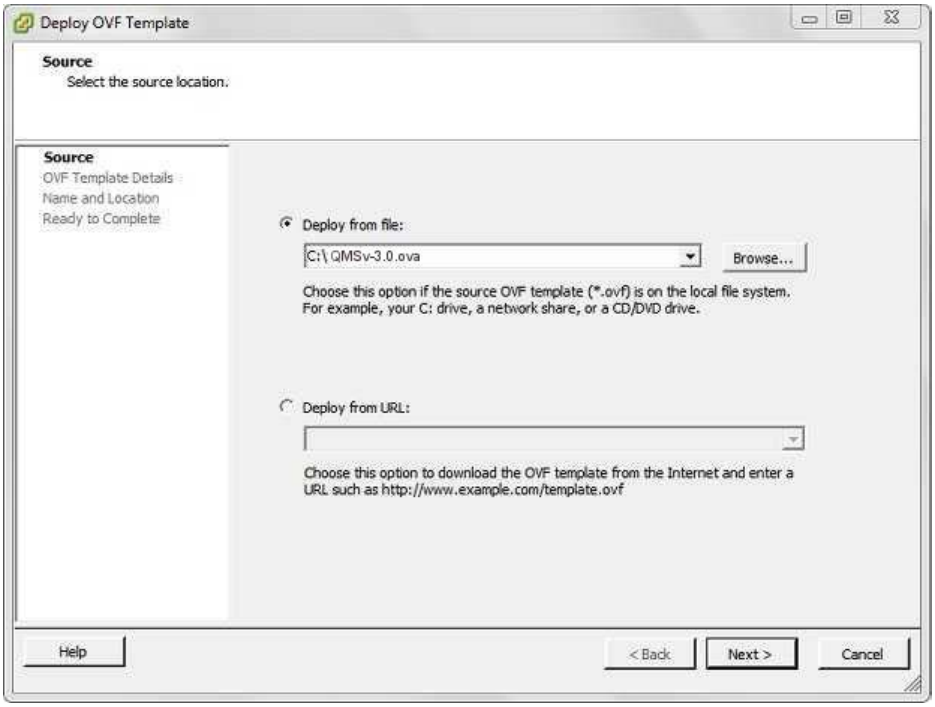
1. Launch the VMware vSphere Client.

2. Type the **IP address**, **User name**, and **Password** for the VMware host, then click **Login**.

## Deploy the QMSv OVF File

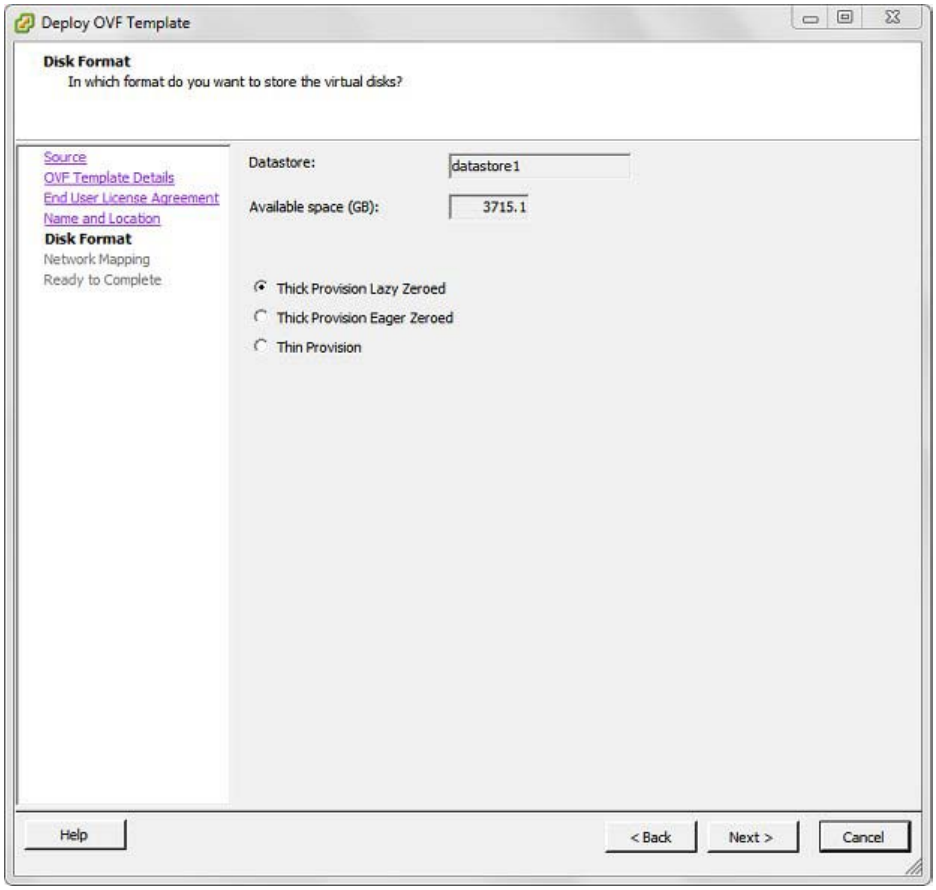
To create the QMSv virtual device, you must deploy the QMSv OVF template in the vSphere client.

1. Launch the vSphere client and log in to the VMware host with administrator credentials.
2. In the vSphere client, select **File > Deploy OVF Template**.


Deploy OVF Template
Source
Select the source location.
Source
OVF Template Details
Name and Location
Ready to Complete
Deploy from file:
C:\ QMSv-3.0.ova
Browse...
Choose this option if the source OVF template (*.ovf) is on the local file system.
For example, your C: drive, a network share, or a CD/DVD drive.
Deploy from URL:
Choose this option to download the OVF template from the Internet and enter a URL such as http://www.example.com/template.ovf
Help
< Back
Next >
Cancel

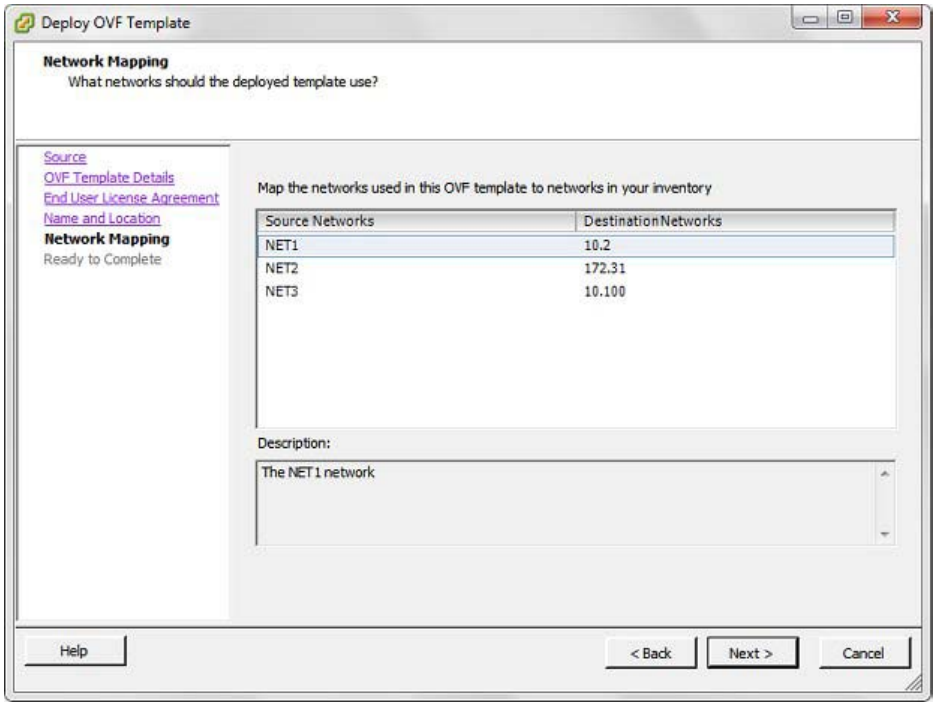
3. **Browse** to the location where you saved the WatchGuard QMSv OVF template file, qmsv-<*version*>.ova. Click **Next**.
   *The QMSv OVF Template Details page appears.*
4. Click **Next**.
   *The End User License Agreement appears.*
5. Review the End-User License Agreement. Click **Accept**. Click **Next**.
   *The Name and Location page appears.*
6. In the **Name** text box, type a name for this virtual device.

7. Select a resource pool within which to deploy this template. Click **Next**.
   *The Disk Format page appears.*



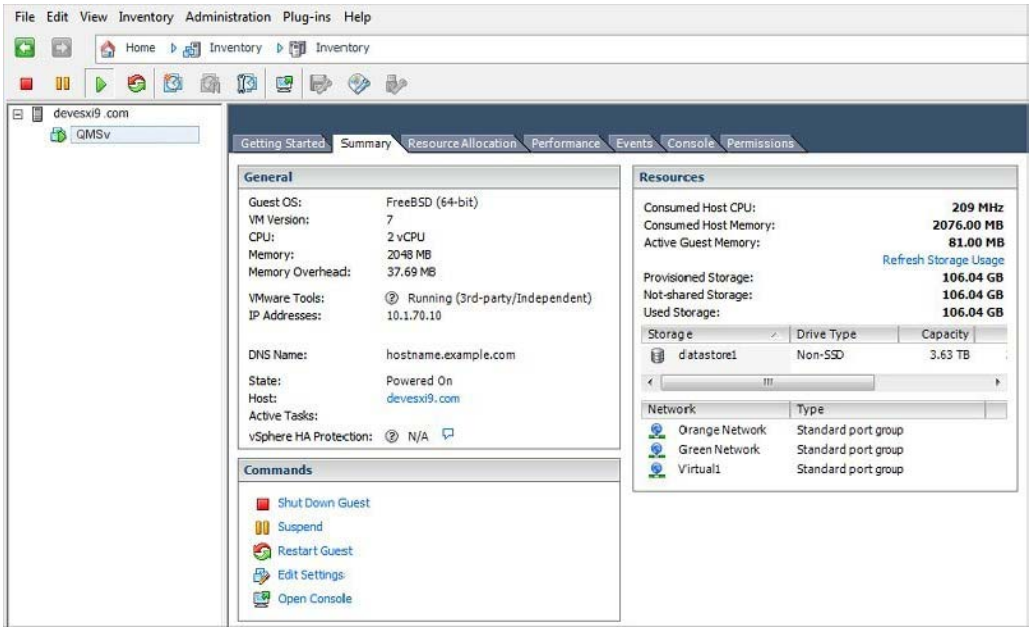

8. Select the format to store the virtual disks. We recommend that you select **Thick provisioned format** to allocate all storage immediately.
9. Click **Next**.
   *The Network Mapping page appears.*

10. In the **Destination Networks** column, select the networks to map to each network interface.




11. Click **Next**.
    *The Ready to Complete page appears.*
12. Review the settings. Click **Back** to change any settings, if necessary.
13. Click **Finish** to deploy the template.
    *The virtual appliance is deployed. This can take a few minutes.*

    The deployed virtual device appears in the vSphere Inventory in the selected resource pool.



## VMware Virtual Machine Resource Allocation

The default WatchGuard QMSv OVF template installation is configured with two virtual CPUs, 2 GB memory, three network adapters, and 80 GB data disk space.

To change your resource settings, you must modify your VMware host resources for virtual processors, memory, and disk space to properly support QMSv installation.

### Configure Virtual CPUs

By default, the QMSv virtual machine is allocated two virtual CPUs.

To modify CPU resources:

1. Launch the vSphere client and log in to the VMware host with administrator credentials.
2. Make sure your QMSv virtual machine is powered off.
3. In the vSphere inventory tree, right click the QMSv virtual machine.
4. Select **Edit Settings**.
5. In the **Hardware** list, select **CPUs**.
6. From the **Number of virtual sockets** drop-down list, select the number of virtual processors.
7. Click **OK**.

### Configure Memory Resources

By default the QMSv virtual machine is allocated 2 GB of memory.

To modify memory resources:

1. Launch the vSphere client and log in to the VMware host with administrator credentials.
2. Make sure your QMSv virtual machine is powered off.
3. In the vSphere inventory tree, right click the QMSv virtual machine.
4. Select **Edit Settings**.
5. In the **Hardware** list, select **Memory**.
6. In the **Memory Size** text box, type or select the memory size.
7. Click **OK**.

### Configure Hard Disk Resources

By default the QMSv virtual device is allocated two hard drives, a primary fixed OS system disk (Hard Disk 1, 24 GB), and a data disk for messages, logs, reports, and quarantine data (Hard Disk 2, 80 GB). You can modify the Hard Disk 2 size and allow for any requirements for additional data disk space for quarantine services..

**! Caution**

Do not modify the Hard Disk 1. This disk is a fixed size and contains the OS for the QMSv.

To increase the size of the Hard Disk 2 data disk:

1. Launch the vSphere client and log in to the VMware host with administrator credentials.
2. Make sure your QMSv virtual machine is powered off.
3. In the vSphere inventory tree, right click the QMSv virtual machine.
4. Select **Edit Settings**.
5. In the **Hardware** list, select **Hard disk 2**.
6. In the **Disk Provisioning** section, modify the **Provisioned Size** setting to the required value.
7. Click **OK**.

To decrease the size of the Hard Disk 2 data disk, you must remove Hard Disk 2 and add a new hard disk:

1. Launch the vSphere client and log in to the VMware host with administrator credentials.
2. Make sure your QMSv virtual machine is powered off.
3. In the vSphere inventory tree, right click the QMSv virtual machine.
4. Select **Edit Settings**.
5. In the **Hardware** list, select **Hard disk 2**.
6. Click **Remove**.
7. Select **Remove from virtual machine and delete files from disk**.
8. Click **OK**.
9. Right click the virtual machine, select **Edit Settings**.
10. Click **Add**.
11. Select **Hard Disk** and click **Next**.
12. Select **Create a new virtual disk** and click **Next**.
13. Set the **Disk Size** to the required value.
14. In the **Disk Provisioning** section, select **Thick Provisioned Lazy Zeroed**.
15. Select **Store with the virtual machine** and click **Next**.
16. In the **Advanced Options**, leave the default settings and click **Next**.
17. Click **Finish**.
18. Click **OK**.

## Start your QMSv Virtual Device

1. In the vSphere Client Inventory tree, select the virtual device.
2. Click the **Summary** tab.
3. In the **Commands** section, select **Power on**.
   *The WatchGuard QMSv virtual device is powered on with factory default settings.*
4. Click the **Console** tab to view the installation process.

**Note**

The WatchGuard QMSv performs an automatic installation. Do not interrupt the installation process.

# Install WatchGuard QMSv

## Default Network Settings

The default network settings for the WatchGuard QMSv after installation are:

- IP address: 10.0.0.1
- Netmask: 255.255.255.0
- Gateway: 10.0.0.2

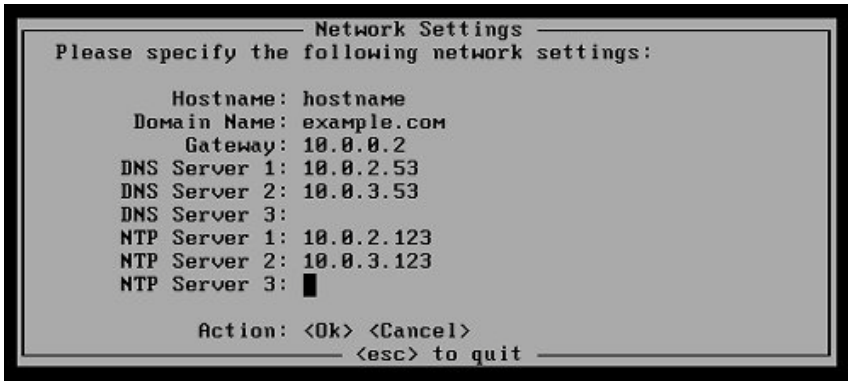
If you want to connect to the QMSv device with the default IP address, go to "Connect to the Setup Wizard" on page 14.

You can change the default IP address of the QMSv and assign the IP addresses of your additional network interfaces before you connect to the Setup Wizard. This allows you to assign IP addresses to the QMSv based on the networks already available on your virtual host system.

To modify the default IP address of your QMSv before running the Setup Wizard:

1. In the vSphere Client Inventory tree, select the QMSv virtual device.
2. Click the **Console** tab.
3. Press **Enter** to display the login screen.

4. Type the default **Username** and **Password**.
   When you access the system for the first time after installation, the default settings are **admin** for the username, and **admin** for the password.
5. On the console menu, select **Admin > Configure Interfaces**.

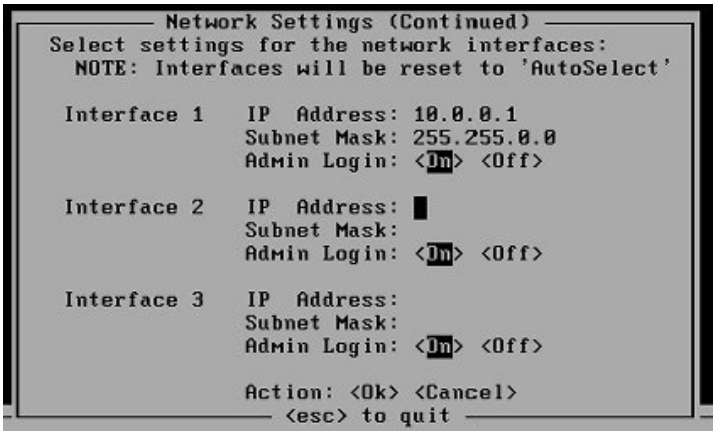



You can configure these options:

- **Hostname** — Type the hostname for the device.
  For example, if your fully qualified domain name is hostname.example.com, type `hostname`.

- **Domain** — Type your domain.
  For this example, type `example.com`.
- **Gateway** — Type the gateway (typically the router) for your network.
  For this example, type `10.0.0.2`.
- **DNS Server** — Type the IP address of your primary and secondary DNS Name Servers.
  For this example, type `10.0.2.53`.
- **NTP Server** — Type the IP address or hostname of your primary and secondary NTP servers.
  For this example, type `10.0.2.123`.

6. Select **OK**.
7. For each network interface, you can configure these options:




- **IP Address** — Type IP address for this interface.
  For this example, type `10.0.0.1`.
- **Subnet Mask** — Type the netmask.
  For this example, type `255.255.255.0`.
- **Admin Login** — Allow administrative access on this interface. You must set this option to **ON** for the interface you will use to access the Setup Wizard.

8. Select **OK**.
9. Select **Yes** to reboot the system.
10. Select **Yes** to confirm.

## Connect to the Setup Wizard

Wait at least five minutes for the system to initialize before you try to connect to the WatchGuard QMSv with a web browser. Ping is enabled on the configured network interface. You can ping the IP address of the QMSv to check connectivity before you connect with a web browser.

**Note**

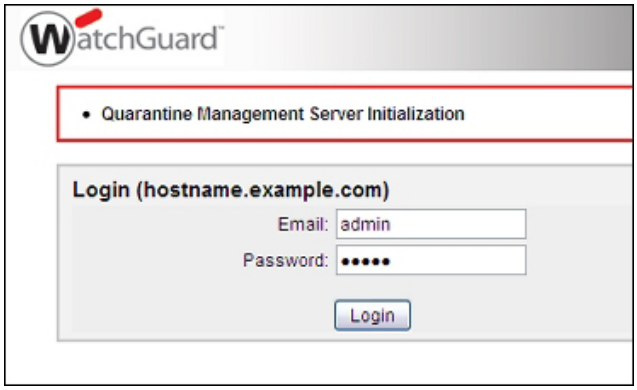
We recommend that you clear your web browser cache before you start the Setup Wizard.

1. Launch a web browser on your computer and type the IP address of the WatchGuard QMSv as the URL in the location bar. For example, `http://10.0.0.1`
   *The login page appears.*

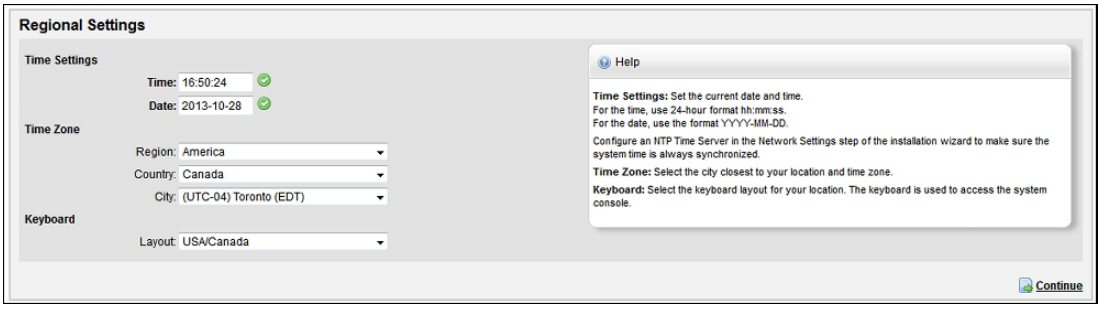
**Note**

A security certificate notification appears in the browser because the system uses a self-signed certificate. It is safe to ignore the warning (Internet Explorer) or to add a certificate exception (Mozilla Firefox).

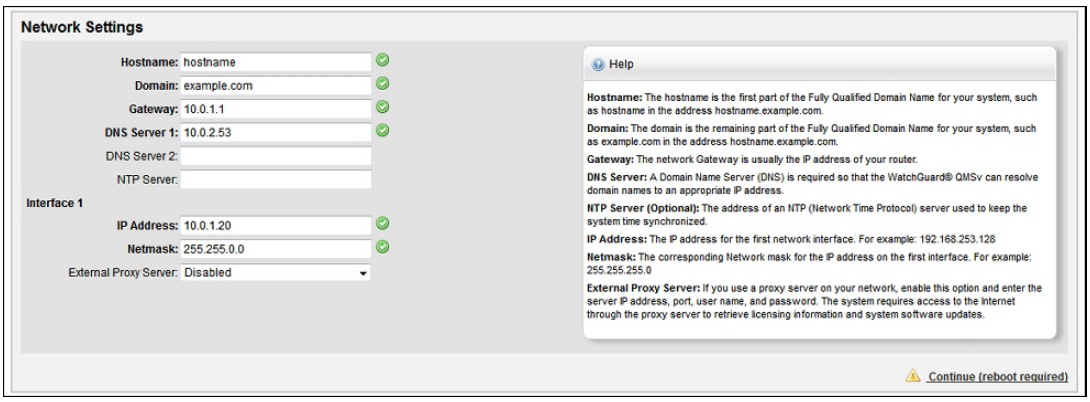
2. Type the default **Username** and **Password**.
   When you access the system for the first time after installation, the default settings are **admin** for the username, and **admin** for the password.




3. The Setup Wizard introduction page appears. Click **Continue** to start the installation.
4. In the **Regional Settings** page, configure these options:
   - **Time Settings** — Type the current **Time** and **Date**. For the time, use 24-hour format hh:mm:ss. For the date, use this format, YYYY-MM-DD.
   - **Time Zone** — Select the closest city to your location and time zone.
   - **Keyboard** — Select the keyboard layout for your location.


Regional Settings
Time Settings
Time: 16:50:24
Date: 2013-10-28
Time Zone
Region: America
Country: Canada
City: (UTC-04) Toronto (EDT)
Keyboard
Layout: USA/Canada
Help
Time Settings: Set the current date and time.
For the time, use 24-hour format hh:mm:ss.
For the date, use the format YYYY-MM-DD.
Configure an NTP Time Server in the Network Settings step of the installation wizard to make sure the system time is always synchronized.
Time Zone: Select the city closest to your location and time zone.
Keyboard: Select the keyboard layout for your location. The keyboard is used to access the system console.
Continue

5. Click **Continue**.
6. On the **Networks Settings** page, configure the first network interface.


Network Settings
Hostname: hostname
Domain: example.com
Gateway: 10.0.1.1
DNS Server 1: 10.0.2.53
DNS Server 2:
NTP Server:
Interface 1
IP Address: 10.0.1.20
Netmask: 255.255.0.0
External Proxy Server: Disabled
Help
Hostname: The hostname is the first part of the Fully Qualified Domain Name for your system, such as hostname in the address hostname.example.com.
Domain: The domain is the remaining part of the Fully Qualified Domain Name for your system, such as example.com in the address hostname.example.com.
Gateway: The network Gateway is usually the IP address of your router.
DNS Server: A Domain Name Server (DNS) is required so that the WatchGuard® QMSv can resolve domain names to an appropriate IP address.
NTP Server (Optional): The address of an NTP (Network Time Protocol) server used to keep the system time synchronized.
IP Address: The IP address for the first network interface. For example: 192.168.253.128
Netmask: The corresponding Network mask for the IP address on the first interface. For example: 255.255.255.0
External Proxy Server: If you use a proxy server on your network, enable this option and enter the server IP address, port, user name, and password. The system requires access to the Internet through the proxy server to retrieve licensing information and system software updates.
Continue (reboot required)

You can configure these options:

- **Hostname** — Type the hostname for the device.
  For example, if your fully qualified domain name is hostname.example.com, type `hostname`.
- **Domain** — Type your domain.
  For this example, type `example.com`.
- **Gateway** — Type the gateway (typically the router) for your network.
  For this example, type `10.0.0.2`.
- **DNS Server** — Type the IP address of your DNS Name Server.
  For this example, type `10.0.2.53`.
- **DNS Server 2** — Type the IP address of a secondary DNS name server.
  For this example, type `10.0.3.53`.
- **NTP Server** — Type the IP address or hostname of your NTP server.
  For this example, type `10.0.2.123`.
- **IP Address** — Type the IP address for this interface.
  For this example, type `10.0.0.1`.
- **Netmask** — Type the netmask.
  For this example, type `255.255.255.0`.
- **External Proxy Server** — If your network uses a proxy server to access the Internet, you must set this option to **Enabled** and enter your external proxy server configuration. The WatchGuard QMSv requires access to the Internet through the proxy server to retrieve licensing information and software updates. If you do not use an external proxy server, leave this option set to **Disabled**.
  - **Server Address** — Type the IP address of your external proxy server.
  - **Server Port** — Type the server port used by the external proxy server. The default is TCP port 80.
  - **User Name** — If your proxy server requires authentication, type the user name to login to the proxy server.
  - **Password** — Type and confirm a password.

7. Click **Continue**.

   If you make any network changes, you must restart the device and reconnect to the WatchGuard QMSv with the new IP address you assigned to the network interface.

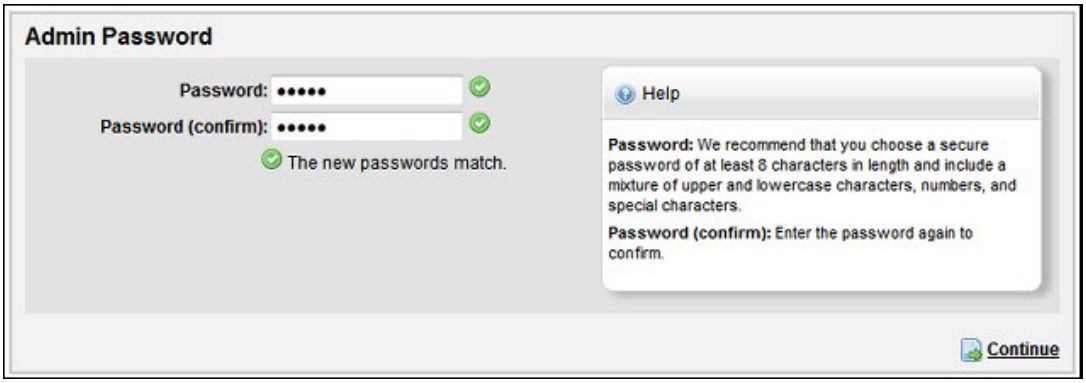
**Note**

Make sure your computer is configured to access the new IP address settings on the WatchGuard QMSv.

8. On the **Customer Information** page, type the **Organization Name** and **Server Admin Email**.
   *Device alerts and notifications are sent to the Server Admin Email address.*

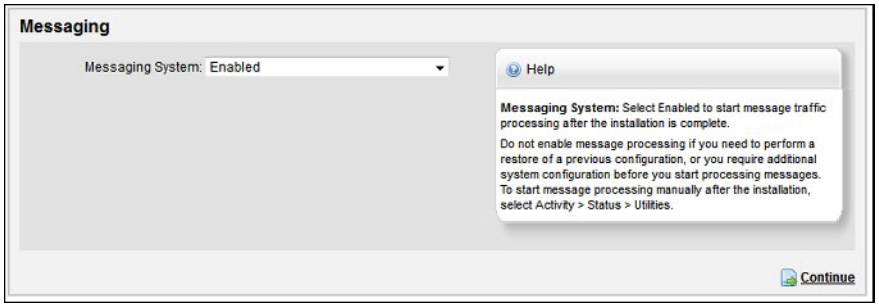
Customer Information
Organization Name: Organization Name
Server Admin Email: admin@example.com
Help
Organization Name: Your company name or web address.
Server Admin Email: The email address used to receive alerts and notifications.
Continue

9. Click **Continue**.
10. On the **Change Password** page, type and confirm a new admin password.
    *We recommend that you choose a secure password of at least 8 characters in length and include a mixture of upper and lowercase letters, numbers, and special characters.*


Admin Password
Password: •••••
Password (confirm): •••••
The new passwords match.
Help
Password: We recommend that you choose a secure password of at least 8 characters in length and include a mixture of upper and lowercase characters, numbers, and special characters.
Password (confirm): Enter the password again to confirm.
Continue

11. Click **Continue**.
12. From the **Messaging System** drop-down list, select **Enabled** to start message traffic processing after the installation is complete.

    If you select **Disabled**, you can start message processing manually from **Activity > Status > Status & Utility** after the installation is complete.


Messaging
Messaging System: Enabled
Help
Messaging System: Select Enabled to start message traffic processing after the installation is complete.
Do not enable message processing if you need to perform a restore of a previous configuration, or you require additional system configuration before you start processing messages. To start message processing manually after the installation, select Activity > Status > Utilities.
Continue

13. Click **Done** to complete the installation.
*This process can take up to a minute to complete.*

Done
Congratulations!
You have completed the basic setup of the WatchGuard® QMSv.
Please click 'Done' to finish the initialization. This process can take up to a minute to complete.
For more information about how to configure your WatchGuard® QMSv, select Support > Online Manual from the Web UI.
Done

# Resource Monitoring

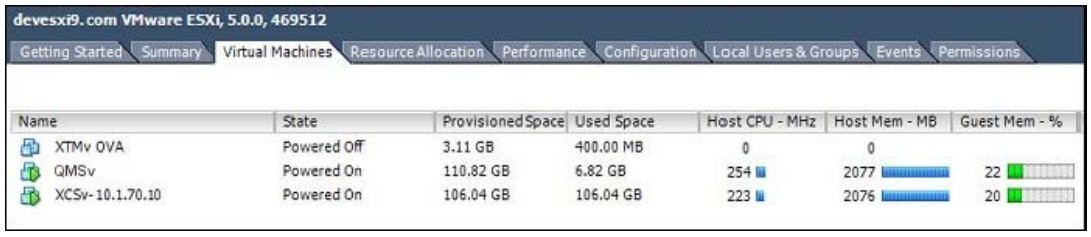
Your virtual host system may host other virtual machines in addition to the WatchGuard QMSv. To ensure that your virtual host resources are properly allocated, you must regularly monitor the resource usage and performance of your virtual host system and your QMSv virtual machine.

## Resource Monitoring on VMware

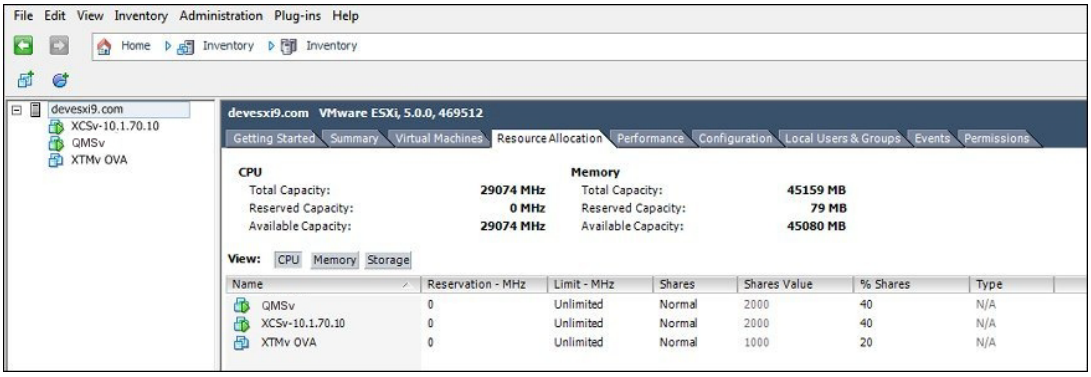
To monitor the resource usage of your VMware host and virtual machines:

1. Launch the vSphere client and log in to the VMware host with administrator credentials.
2. In the vSphere inventory tree, select your VMware host system at the top of the list.
3. Select the **Virtual Machines** tab.

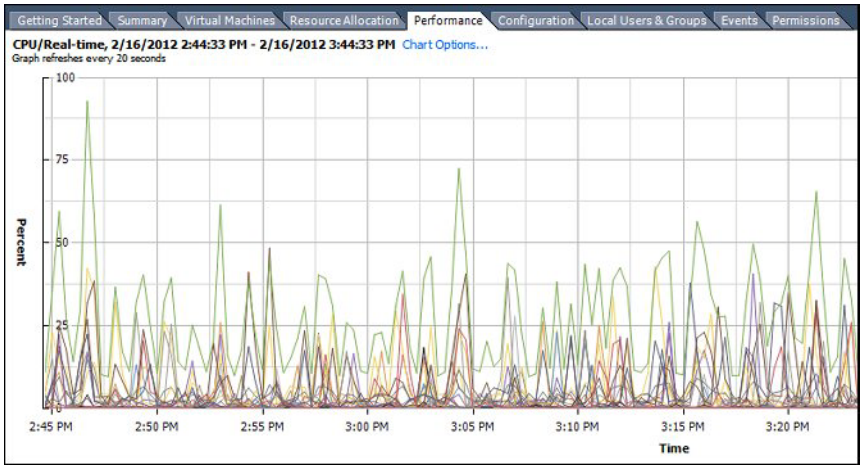
   You can view the disk space, CPU usage, and memory utilization of each virtual machine hosted on your VMware system.



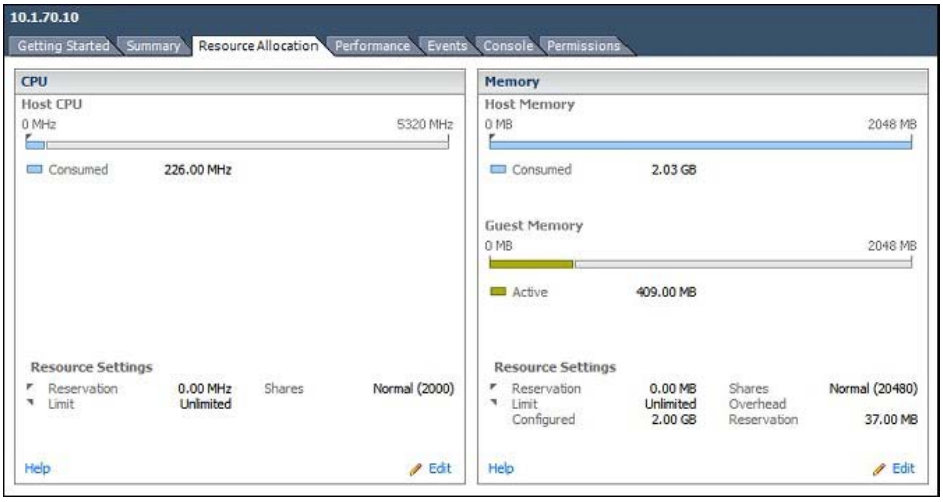

4. Select the **Resource Allocation** tab.
5. You can switch between **CPU**, **Memory**, and **Storage** view for a more detailed examination of the resources used by your virtual machines on the VMware host.



6. Select the **Performance** tab for a customized chart view of the VMware host performance.




7. In the vSphere inventory tree, select your QMSv virtual machine.
8. Select the **Resource Allocation** tab.
   You can examine the resources in use specifically by the QMSv virtual machine.




9. Select the **Performance** tab for a customized chart view of the QMSv virtual machine performance.